AMENDMENTS/REMARKS

Applicant has reviewed and considered the final Office Action dated December 2, 2002. Claims 1-43 were pending in the present application. It is noted that although the pending Office Action makes reference to claim 44, Applicant's response to the prior Office Action corrected the numbering of claims 38-44, renumbering them as claims 37-43, because no claim 37 existed in the claims as filed. Thus, claims 1-43 are pending. However, new claims are added in this Amendment for consideration and, for clarity, claims 1-44 have been cancelled so that new claims 45-70 can be added.

Rejections under 35 U.S.C. § 103(a)

Claims 1, 15, and 30 were rejected under 35 U.S.C. § 103(a) as being anticipated by U.S. patent No. 6,128,661 to Yanagidate. Applicant respectfully disagrees with the rejection for at least the following reasons.

Background

The present invention operates within a limitation inherent in current IP addressing and provides a solution to facilitate peer-to-peer application communication in that addressing environment. There is a limited universe of global IP addresses in the present Internet. The number of applications (or terminals, to use Yanigadate's terminology) in networks connected to the Internet that desire to communicate using the Internet's global IP addresses exceeds the limited universe of global IP addresses. Thus, private networks with private address realms have been developed to carry messages within the private address realm. These addresses in the private address realm may overlap with addresses in the external or global IP address realm. Thus, to avoid confusion and misdirected messages, the private addresses are valid only in the private network/private address realm. To enable communication from applications/terminals within the private address realm to applications/terminals outside the private address realm and vice versa, the private address realm may have associated with it a set of available addresses valid outside the private address realm, i.e., valid and available for use in the external or global IP address realm.

When an application/terminal within the private address realm is to communicate with an application/terminal outside the private address realm, that application requires use of one of the

set of available addresses valid outside the private address realm, i.e., in the external or global address realm. This use is facilitated by associating the application's private address with an assigned address valid outside the private address realm, i.e., in the global address realm. The association is called a translation rule, because any message incoming from the external address realm and directed to the application will have as the destination address the assigned external address instead of the private address. In a network that uses a Network Address Translator or NAT, it is the NAT that implements the translation rule. To cause the external message to reach the application, the NAT must translate that destination address (the assigned external address) into the associated private address so that the private address network can direct the message to the application that holds the temporary assignment for that external address. A NAT performs such translation by operating on the IP address fields of the message packets.

As explained at pages 4-6 of applicant's specification, a conventional NAT operates and applies translation rules in one of two modes, depending on whether the message requiring translation is incoming or outgoing. In the case of outgoing messages, the NAT examines the source address and port of the initial packet of a data transaction, which identify the internal application initiating the packet, using internal address information. The NAT then chooses an address from the available set of externally valid IP addresses and associates that with the internal address information. The NAT finally modifies the outgoing message packet to insert as the source address the chosen, externally-valid IP address. This permits the application that receives the message to reply by using the source address in the message packet as the destination address (externally valid) for the return message.

In the case of incoming messages, a conventional NAT uses fixed internal-external address correspondence information, defined by the person administering the NAT. The NAT at the target organization for the incoming message examines the destination address of the incoming message. It consults its configuration information to find the corresponding internal address and port number. It then substitutes the internally valid address information for the destination address of the incoming message and passes the message packet to the internal network, where that internal address information will be used to direct the message to the correct application.

Yanagidate Reference

The Yanagidate reference shows a NAT 14 that is associated with a private address realm/network 12. It further shows that this NAT 14 performs the translation from an incoming global or external address to a private address. When an application/terminal 11a outside the NAT wants to communicate to an application 12a or 12b within the NAT and the application is known by its host name, the outside application asks the NAT 14 for the global address of the application within the NAT. The application outside the NAT sends an IP message to the NAT over router 12, because that is the only way it can communicate to the NAT. Yanagidate teaches how the NAT 14 responds by finding the private address associated with the host name and then finding any assigned global IP address associated with the private address. If there is no assigned global address, then the NAT automatically makes the global address-private address assignment (temporarily) and reports the assigned global address to the outside or global application /terminal 12a. Thus, the address is requested by an application outside the private address realm and the address selected and returned to the outside application is a global address from the set of global address that are available for assignment to an application within the private network. The address request is made by the outside application providing a host name in an IP message packet directed to the NAT.

The NAT in Yanagidate assumes that there are a limited number of global IP addresses available for assignment by the NAT and therefore uses a timing scheme to keep track of the last access time and, after a predetermined time period, deletes a private address-global IP address pair that the NAT has established. While this alleviates the problem of sharing the limited number of IP addresses assigned to the private address realm 12, Yanagidate's only teaching is that an inquiry from the global address realm 11 by providing a host name leads to a temporary pairing of a global IP address with a particular host name and private address. Given the way a conventional NAT functions, the temporary address pairing developed by the NAT at the instigation of an inquiry message packet from the global address realm is beyond the control of the application/terminal having the private address in the pairing in at least two ways. First, the application with the private address does not initiate the assignment. Second, the assigned external address is reported, not to the private application/terminal 12a or 12b, but to the inquiring external application/terminal 11a.

Applicant's NAT

By contrast, although the present invention shows a NAT 320 and this NAT performs the translation from an incoming global or external address to a private or internal address, the function is quite different. The NAT 320 serves address realm 100, which connects to the global internet address realm 400, which in turn connects to another address realm 200. The control channel 350 and the address manager 324 of applicant's NAT are not configured to respond to an address inquiry incoming from either of the address realms 400 or 200 outside of address realm 100 as in Yanagidate. Rather, as seen in Fig. 3, the control channel 350 and address manager 324 are set up for control communications with an application 121, 122 within Host A in address realm 100.

Applicant recognized that in peer to peer situations, it is advantageous for an application within the private address realm served by a NAT to have a more sophisticated relationship to the NAT than simply having the NAT automatically consult its translation rules and rewrite the address fields in message packets or, as in Yanagidate, to have the NAT respond to an outside application's request for an external address corresponding to a host name tied to an internal address. In applicant's invention the control channel 350 and address manager 324 provide a flexible facility for applications served by the NAT to get information they do not get from a conventional NAT and have the power to influence the NAT's translation rules, using the set of externally valid addresses available to applications served by the NAT.

As described at pages 15-16 of applicant's specification, the control channel 350 is used when an application on Host A or any other host served by the NAT 320 needs to communicate with the NAT to request services of the address manager 324. The address manager 324 can perform several services for a requesting application served by NAT 320.

1. The NAT can provide an application on Host A with one of the externally valid IP addresses that is available for network 100 as part of a translation pair rule that the NAT will use. Unlike in Yanagidate, this externally valid IP address is obtained as a result of a communication from an application within the private address realm served by the NAT. The communication occurs over the control channel 324 internal to the NAT, and the NAT responds back to the requesting application within its address realm, not to an outside application. The NAT establishes the translation pair rule and then provides the application with that one of the external

addresses available to the address realm served by the NAT and used in the rule. That is, the inquiry comes from the internal or private address realm served by the NAT and the NAT's response is to that internal address realm, not to another address realm, as in Yanagidate. This is significant because communicating that address to the application over the control channel 350, puts the requesting application in the position where it can send its own address as data to another application. The application may then control communication of its externally valid address regardless of what the NAT (or any other routing device) does with addresses in the message headers of an outgoing message packet.

2. In requesting an available external address, the application on Host A can cause the address manager 324 to provide an available address with required or desired characteristics. This can be useful to let an application specify that the external IP address that will result from translation of the application's internal address will be a particular address or within a specified range of address. Thus, the application can by its address request over the control channel 350 cause the NAT to establish a translation rule that will cause a message packet outgoing from Host A to be forced to a particular external server. This server could then direct the message to any particular private network, before the message packet is finally forwarded again to the public global Internet.

3. The communication from the application on Host A over the control channel 350 to the address manager 324 can request the address manager 324 to establish not just a simple internal-external address pairing rule for translation but rather a more complex rule. The table of address associations could be set up with a contingency, whereby the address translation section 322 checks the incoming source address and/or port and applies a different translation rule depending on the content of the source address field. That is, the application can control the internal path of incoming messages by specifying over control channel 350 that one translation of the externally valid destination address in the header of an incoming message be used if the source address meets certain criteria and another translation be used if the criteria are not met. See applicant's specification at 15-16.

None of this interaction of a NAT and an application internal to network served by the NAT, using a control channel to specify translation rules, is taught by Yanagidate, because Yanagidate deals only with simple address translation pairing, responsive to a request

from an application/terminal outside a private network. The outside terminal has only IP message packet communication with the NAT that serves the private network. In contrast to Applicant's invention, in Yanagidate the address-translating connection device handles an address request that comes from the global or external address realm. As stated in the Abstract:

> An address-translating connection device which makes it possible to dynamically assign an IP address to a private address when a connection is made to inside of a LAN from outside.

Yanagidate, Abstract, first sentence (emphasis added). There is no motivation or suggestion in Yanagidate that its address lookup table and IP address control table be used to establish a translation rule, except "when a connection is made to inside of a LAN from outside." In Applicant's invention, there is a control channel 350 that permits an application within the private network to affect the behavior of the NAT, both to influence the translation rules and to get access to address information that the NAT normally holds in its tables for message header address translation but does not make available to internal applications.

Applicant's invention deals with communication between entities in disparate address realms. They are disparate in that communication from one address realm to the other only occurs if a message sent across the boundary between the two realms has an address valid in the receiving realm. This can occur between two private networks that may have overlapping addresses, in which case an internal address in one private network must be translated into an address that is unique and valid when it is used externally, i.e., in the other network. It can also occur between a private network with private or internal addresses and a public, external network, such as the Internet, in which unique and properly assigned IP addresses must be used. Thus, the terms "internal address" or "private address" and "external address" "or global address" refer to two different sides of a boundary between two disparate address realms, from the viewpoint of one side. A frequent example is the situation show in Yanagidate, where there is a private network that connects to the global IP network and the private network has available a limited set of externally valid IP addresses. However, the present invention is applicable to any network address translation facility on one side of an address realm boundary that provides control services to the applications on the same side of such boundary.

Accordingly, Applicant respectfully submits that new independent claims 45 and 58 patentably distinguish over Yanagidate. The respective dependent claims, also rejected under 35 U.S.C. 103(a) in view of Yanagidate, are distinguishable as well, a fortiori because of their additional features. With regard to dependent claims 49-50 and 62-63, it is submitted that Yanagidate only shows a single address for any terminal and therefore does not teach requesting either a terminating address or an originating address.

With regard to claims 54-55 and 67-68 and the position stated in the final Office Action for claims 9, 24 and 39 (relating to peer-to-peer communication), it is submitted that reference number 14a does not identify a terminal but rather a table in address translating device 14. Thus, the argument that "the communication between terminal 11a and terminal 14a uses the same IP protocol layer" has an incorrect foundation and cannot support the rejection. Moreover, it is not seen how Fig. 2 of Yanagidate shows a common protocol layer. In addition, applicant's reference to peer-to-peer communication is based on the definition at page 9 of the specification, not on protocol layers and, as to claims 55 and 68, Yanagidate lacks any mention of telephony.

With regard to claims 47-48, 56-57, 60-61 and 69-70, it is submitted that Yanagidate has no teaching whatsoever of an application specifying a particular a forced address association or a contingent translation rule. The Office Action asserts that such matters are obvious to a person skilled in the art; however, this assertion is not supported by any citation to Yanagidate or any other prior art.

The remaining dependent claims not specifically discussed above are distinguishable for at least the same reasons as independent claims 45 and 58. Reconsideration and withdrawal of all rejections based on 35 U.S.C. 103(a) in view of Yanagidate is respectfully requested.

CONCLUSION

In view of the above, it is respectfully submitted that the present application is in condition for allowance. Reconsideration of the present application and a favorable response are respectfully requested.

If a telephone conference would be helpful in resolving any remaining issues, please contact the undersigned at (612) 340-2734.

Respectfully submitted,

DORSEY & WHITNEY LLP

Date: June 2, 2003

By: _____

Stuart R. Hemphill (Reg. No. 29,084)
Suite 1500
50 South Sixth Street
Minneapolis, MN 55402-1498
(612) 340-2734
Attorneys for Applicant